JOURNALCTL CHEAT SHEET
(DFIR EDITION)

Hal Pomeranz
hrpomeranz@gmail.com
v1.0.1

BEFORE YOU START

`export SYSTEMD_PAGER=`

Set SYSTEMD_PAGER to null so that output lines wrap instead of scrolling.

`journalctl -D /path/to/directory`
`journalctl --file=somefile`

Journal logs are normally found under `/var/log/journal/MACHINE_ID`
Use the `-D` switch to specify an alternate directory, or `--file` to select individual files

`journalctl --header`

Summarizes information from each journal file. Includes first/last dates, boot number, number of objects, etc.

OUTPUT MODES

`-q -o short`

Syslog-style output w/o extra header

`-q -o short-iso --utc`

Better timestamp, force UTC output

`-o json`

Single line JSON, for script processing

`-o json-pretty`

Multi-line JSON for readability

SIMPLE SEARCH CRITERIA

`--facility=`*`name`*

Search by Syslog facility name

`-u `*`name`*`.service`

Search by Systemd unit name

`-t `*`identifier`*

Match SYSLOG_IDENTIFIER field

`-g `*`regex`*

PCRE match against log message text

SPECIFY TIME RANGES

`-S, --since`
`-U, --until`

Search after/before specified time

Sample time specifiers:

```
-S 2024-08-07 09:30:00
-S 2024-07-24
-U yesterday
-U “15 minutes ago”
-S -1hr
-S 2024-07-24 -U yesterday
```

OTHER FIELDS

`journalctl -N`

List all field names found in journal

`journalctl -F `*`field`*

List all values found for given field

`journalctl `*`FIELD=value`*

Match entries where named *`FIELD`* equals chosen *`value`*

EXAMPLE COMMANDS

`journalctl -q -o short --facility=authpriv`

Recreate `/var/log/auth.log`

`journalctl -q -o short-iso -u ssh -g Accepted`

Who is logging in with SSH and from where?

`journalctl -q -o short-iso _UID=1000`

Find messages related to a given user ID

`journalctl -q -o short-monotonic --dmesg`

Recreates traditional `dmesg` output

`journalctl -q -o short-iso -t sudo -g COMMAND= -r`

Pull interesting Sudo-related messages, most recent first (`-r`)

`journalctl -q -o short-iso -f`

On live system, show continuous logs (like `tail -f`), Ctrl-C aborts